



# UNITED STATES PATENT AND TRADEMARK OFFICE

*cm*

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/674,286	09/29/2003	Biing-Hwang Juang	502076-A-01-US (Juang)	3118
47702 7590 04/18/2007 RYAN, MASON & LEWIS, LLP 1300 POST ROAD SUITE 205 FAIRFIELD, CT 06824			EXAMINER LENNOX, NATALIE	
			ART UNIT 2609	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE		MAIL DATE	DELIVERY MODE	
3 MONTHS		04/18/2007	PAPER	

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

# Office Action Summary

Application No.

10/674,286

Applicant(s)

JUANG ET AL.

Examiner

Natalie Lennox

Art Unit

2609

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 29 September 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on February 23, 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

### ***Claim Rejections - 35 USC § 101***

1. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 16-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

With respect to claims 16-20, Applicant claims an article of manufacture for authenticating a user comprising a "machine readable medium". In accordance with Applicant's specification the machine or computer readable medium may be a transmission medium including the use of a wireless channel or radio frequency channel. This subject matter is not limited to that which falls within a statutory category of invention because it is not limited to a process, machine, manufacture, or a composition of matter. Instead, it includes a form of energy. Energy does not fall within a statutory category since it is clearly not a series of steps or acts to constitute a process, not a mechanical device or combination of mechanical devices to constitute a machine, not a tangible physical article or object which is some form of matter to be a product and constitute a manufacture, and not a composition of two or more substances to constitute a composition of matter. Claims 16-20 are also rejected since they produce no tangible result. An example of a tangible result would be using the processed information to determine if the claimed user is the user indeed, or using the processed information to allow or deny access to a system.

***Claim Rejections - 35 USC § 102***

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 5, 9, 13, 16, and 18 are rejected under 35 U.S.C. 102(e) as being anticipated by Ramaswamy et al. (US Patent 6,490,560).

As per claim 1, Ramaswamy et al. teach a method for authenticating a user, comprising:

obtaining an asserted identity of said user (Col. 4, lines 55-59, *The verification process may include matching an acoustic signature of the person claiming to be a given user to the known acoustic signature of the claimed user*);

presenting one or more questions to said user that said user has previously answered (Col. 4, lines 59-63, *The verification process may also include biometric verification whereby the person claiming to be the user is prompted for answers to specific questions, such as password, mother's maiden name, social security number, etc.*, it is inherent that these questions had been previously answered for the system to be able to compare results); and

processing spoken answers to said one or more questions using an automatic speech recognition technique (Col. 4, lines 15-20, *The input from the user is expected*

*to be a spoken utterance [...] When a spoken input is used, a conversational system first converts the spoken utterance into text using a speech recognition engine).*

As per claim 5, Ramaswamy et al. teach the method according to claim 1, wherein said processing step further comprises the step of converting said spoken answers to a textual form and comparing said textual form to answers obtained during an enrollment phase (Col. 4, lines 18-20, *When spoken input is used, a conversational system first converts the spoken utterance into text using a speech recognition engine*, also in Col. 4, lines 55-63, *The verification process may include matching an acoustic signature of the person claiming to be a given user [...] The verification process may also include biometric verification whereby the person claiming to be the user is prompted for answers to specific questions, such as password, mother's maiden name, social security number, etc.*, just as stated in lines 55 to 59, part of the verification process includes matching or comparison, and as stated before it is inherent that the answers for the specific questions had been already answered in order for the system to be capable of comparing results).

As per claim 9, Ramaswamy et al. teach an apparatus for authenticating a user, comprising:

a memory (Col. 3, lines 52-57, *these elements are implemented in software on one or more appropriately programmed general purpose digital computers having a processor and memory and input/output interfaces*); and

at least one processor, coupled to the memory (Col. 3, lines 52-57, *these elements are implemented in software on one or more appropriately programmed*

*general purpose digital computers having a processor and memory and input/output interfaces), operative to:*

obtain an asserted identity of said user (Col. 4, lines 55-59, *The verification process may include matching an acoustic signature of the person claiming to be a given user to the known acoustic signature of the claimed user*);;

present one or more questions to said user that said user has previously answered (Col. 4, lines 59-63, *The verification process may also include biometric verification whereby the person claiming to be the user is prompted for answers to specific questions, such as password, mother's maiden name, social security number, etc., it is inherent that these questions had been previously answered for the system to be able to compare results*); and

process spoken answers to said one or more questions using an automatic speech recognition technique (Col. 4, lines 15-20, *The input from the user is expected to be a spoken utterance [...] When a spoken input is used, a conversational system first converts the spoken utterance into text using a speech recognition engine*).

As per claim 13, Ramaswamy et al. teach the apparatus according to claim 9, wherein said processor is further configured to convert said spoken answers to a textual form and comparing said textual form to answers obtained during an enrollment phase (Col. 4, lines 18-20, *When spoken input is used, a conversational system first converts the spoken utterance into text using a speech recognition engine*, also in Col. 4, lines 55-63, *The verification process may include matching an acoustic signature of the person claiming to be a given user [...] The verification process may also include*

Art Unit: 2609

*biometric verification whereby the person claiming to be the user is prompted for answers to specific questions, such as password, mother's maiden name, social security number, etc., just as stated in lines 55 to 59, part of the verification process includes matching or comparison, and as stated before it is inherent that the answers for the specific questions had been already answered in order for the system to be capable of comparing results).*

As per claim 16, Ramaswamy et al. teach an article of manufacture for authenticating a user, comprising a machine readable medium containing one or more programs which when executed implement the steps of (Col. 3, lines 52-54):

obtaining an asserted identity of said user (Col. 4, lines 55-59, *The verification process may include matching an acoustic signature of the person claiming to be a given user to the known acoustic signature of the claimed user*);

presenting one or more questions to said user that said user has previously answered (Col. 4, lines 59-63, *The verification process may also include biometric verification whereby the person claiming to be the user is prompted for answers to specific questions, such as password, mother's maiden name, social security number, etc., it is inherent that these questions had been previously answered for the system to be able to compare results*); and

processing spoken answers to said one or more questions using an automatic speech recognition technique (Col. 4, lines 15-20, *The input from the user is expected to be a spoken utterance [...] When a spoken input is used, a conversational system first converts the spoken utterance into text using a speech recognition engine*).

As per claim 18, Ramaswamy et al. teach the article of manufacture according to claim 16, wherein said processing step further comprises the step of converting said spoken answers to a textual form and comparing said textual form to answers obtained during an enrollment phase (Col. 4, lines 18-20, *When spoken input is used, a conversational system first converts the spoken utterance into text using a speech recognition engine*, also in Col. 4, lines 55-63, *The verification process may include matching an acoustic signature of the person claiming to be a given user [...] The verification process may also include biometric verification whereby the person claiming to be the user is prompted for answers to specific questions, such as password, mother's maiden name, social security number, etc.*, just as stated in lines 55 to 59, part of the verification process includes matching or comparison, and as stated before it is inherent that the answers for the specific questions had been already answered in order for the system to be capable of comparing results).

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 2, 3, 6, 10, 11, 14, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ramaswamy et al. (US Patent 6,490,560) as applied to claims 1, 9, and 16 above, and further in view of Honarvar et al. (US 2003/0154406).



As per claim 2, Ramaswamy et al. teach the method and apparatus according to claim 1, but they don't specifically mention said processing step being performed until a predefined security threshold is satisfied. However, Honarvar et al. teach that in order to develop a confidence score, for example, for an identity verification sub-process, a vendor determines the points for each authentication question to derive predictive confidence scores. A predictive confidence score is a threshold that indicates whether the vendor's organization feels the user has been authenticated sufficiently enough to proceed with a business transaction (Paragraph [0233]).

It would have been obvious to one having ordinary skill in the art to have combined the feature of a security threshold as taught by Honarvar et al. with Ramaswamy et al.'s method because Honarvar et al. provides a method for user authentication where the authentication result is determined by calculating a confidence score based upon the parameters assigning points to each generated authentication question (Paragraph [0041]).

As per claim 3, Ramaswamy et al., as modified above, teach the method according to claim 2, wherein said predefined security threshold is based on a sum of security weights of correctly answered questions (Honarvar et al.'s paragraphs [0233] and [0234], where *the confidence score is a threshold that indicates whether the vendor's organization feels the user has been authenticated sufficiently enough to proceed with a business transaction. Questions weighing involves the assigning of point values to all of the questions that comprise an authentication sub-process of a user authentication process. The authentication engine generates a confidence score*

*upon completion of the identity verification sub-process [and] determines which questions are answered correctly and totals the associated points for each correct response).*

As per claims 6 and 19, Ramaswamy et al. teach the method and article of manufacture according to claims 1 and 16, but don't specifically mention said processing step further comprising the step of obtaining a confidence score for a recognized version of said spoken answer. However, Honarvar et al. teach a confidence score, for example, for an identity verification sub-process, a vendor determines the points for each authentication question to derive predictive confidence scores, and that the questions weighing involves the assigning of point values to all of the questions that comprise an authentication sub-process of a user authentication process. The authentication engine determines which questions are answered correctly and totals the associated points for each correct response (Paragraphs [0233] and [0234]).

It would have been obvious to one having ordinary skill in the art to have combined the feature of a security threshold as taught by Honarvar et al. with Ramaswamy et al.'s method and article of manufacture because Honarvar et al. provides a method and article of manufacture for user authentication where the authentication result is determined by calculating a confidence score based upon the parameters assigning points to each generated authentication question (Paragraph [0041]).

As per claim 10, Ramaswamy et al. teach the apparatus according to claim 9, but they don't specifically mention said processor being further configured to process said spoken answers until a predefined security threshold is satisfied. However, Honarvar et al. teach that in order to develop a confidence score, for example, for an identity verification sub-process, a vendor determines the points for each authentication question to derive predictive confidence scores. A predictive confidence score is a threshold that indicates whether the vendor's organization feels the user has been authenticated sufficiently enough to proceed with a business transaction (Paragraph [0233]).

It would have been obvious to one having ordinary skill in the art to have combined the feature of a security threshold as taught by Honarvar et al. with Ramaswamy et al.'s apparatus because Honarvar et al. provides a method and system for user authentication where the authentication result is determined by calculating a confidence score based upon the parameters assigning points to each generated authentication question (Paragraph [0041]).

As per claim 11, Ramaswamy et al., as modified above, teach the apparatus according to claim 10, wherein said predefined security threshold is based on a sum of surety weights of correctly answered questions (Honarvar et al.'s paragraphs [0233] and [0234], where *the confidence score is a threshold that indicates whether the vendor's organization feels the user has been authenticated sufficiently enough to proceed with a business transaction. Questions weighing involves the assigning of point values to all of the questions that comprise an authentication sub-process of a user authentication*

*process. The authentication engine generates a confidence score upon completion of the identity verification sub-process [and] determines which questions are answered correctly and totals the associated points for each correct response).*

As per claim 14, Ramaswamy et al. teach the method according to claim 9, but they don't specifically mention said processor being further configured to obtain a confidence score for a recognized version of said spoken answer. However, Honarvar et al. teach that in order to develop a confidence score, for example, for an identity verification sub-process, a vendor determines the points for each authentication question to derive predictive confidence scores, and that the questions weighing involves the assigning of point values to all of the questions that comprise an authentication sub-process of a user authentication process. The authentication engine determines which questions are answered correctly and totals the associated points for each correct response (Paragraphs [0233] and [0234]).

It would have been obvious to one having ordinary skill in the art to have combined the feature of a security threshold as taught by Honarvar et al. with Ramaswamy et al.'s apparatus because Honarvar et al. provides an apparatus for user authentication where the authentication result is determined by calculating a confidence score based upon the parameters assigning points to each generated authentication question (Paragraph [0041]).

6. Claims 4, 7, 12, 15, 17, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ramaswamy et al. (US Patent 6,490,560) as applied to claims 1, 9, and 16 above, and further in view of August (US 2002/0094067).

As per claims 4, 12, and 17, Ramaswamy et al. teach the method, apparatus, and article of manufacture according to claims 1, 9, and 16, but don't specifically mention further comprising the step of processing said answer using an utterance verification technique. However, August teaches a speech processing unit that includes an Utterance Verification/Verbal Information Verification (VIV) application. The VIV application enables the network to interpret spoken utterances of a subscriber (Paragraph [0048]).

It would have been obvious to a person having ordinary skill in the art to have combined August's feature of an utterance verification application for Ramaswamy et al.'s method, apparatus, and article of manufacture because August provides an automated speech recognition method and system such as Verbal Information Verification or the like that has the flexibility to utilize a more extensive grammar than in a system recognizing only globally-available commands without having to train the system to recognize the particular subscriber's pronunciations of words (Paragraph [0012]).

As per claims 7, 15, and 20, Ramaswamy et al. teach the method, apparatus, and article of manufacture according to claims 1, 9, and 16. Ramaswamy et al. also teach a verification process that may include biometric verification whereby the person claiming to be the user is prompted for answers to specific questions, such as a

Art Unit: 2609

password, mother's maiden name, social security number, etc. (Col. 4, lines 59-63), where it is inherent that the questions had to be already answered by the user in order for the verification process to be able to compare them. Ramaswamy et al. don't specifically mention the processing step further comprising or processor further configured to employ word spotting techniques. However, August teaches a signal processing unit that processes an acoustic signal using word spotting and utterance verification with Verbal Information Verification (VIV) to recognize the recited words (Paragraph [0065]).

It would have been obvious to a person having ordinary skill in the art to have combined August's feature of a word spotting technique for Ramaswamy et al.'s method, apparatus, and article of manufacture because August provides an automated speech recognition method and system such as Verbal Information Verification or the like that has the flexibility to utilize a more extensive grammar than in a system recognizing only globally-available commands without having to train the system to recognize the particular subscriber's pronunciations of words (Paragraph [0012]).

7. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ramaswamy et al. (US Patent 6, 490,560) as applied to claim 1 above, and further in view of Arnold (US 2002/0147914).

As per claim 8, Ramaswamy et al. teach the method according to claim 1, but don't specifically mention said authentication being performed in connection with the resetting of a password of said user. However, Arnold teaches that once the user has been authenticated, the automated password reset program resets the password and

Art Unit: 2609

delivers a new password to the user in a way that further enhances the overall security of the system (Paragraph [0010]).

It would have been obvious to one having ordinary skill in the art to have combined the feature of a resetting of a password as taught by Arnold for Ramaswamy et al.'s method because Arnold provides a method of providing a password reset without the use of human intervention, a way to provide a new password without introducing a delay between resetting the password and the user actually receiving the new password, and a technique to deliver the new password to the user in a way that further enhances the security of the system (Paragraph [0008]).

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Natalie Lennox whose telephone number is (571) 270-1649. The examiner can normally be reached on Monday to Friday 7:30 am - 5:00 pm (EST).


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Xiao Wu can be reached on (571) 272-7761. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2609

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NL

04/12/2007

  
XIAO WU  
SUPERVISORY PATENT EXAMINER